SY402 1131 Lab 7: Ensuring Host Integrity

1. What did inotify-tools provide?
   1. inotify-tools: command-line programs providing a simple interface to inotify
2. What files/directories does the system ignore, and are there any that it specifically tracks?
   1. Files can be ignored manually in the configuration or using rules. By default when a file has changed 3 times further changes are automatically ignored.
   2. Default: /etc/mtab
3. By default, for how long does OSSEC block traffic that triggers a firewall rule?
   1. firewall-drop enabled (local) for levels >= 6
   2. The IP is going to be blocked for 600 seconds.
4. By default, How often does OSSEC check for new files? Can OSSEC detect file changes in realtime? If so, how do you configure OSSEC to set the important directories?
   1. By default integrity checking occurs every 6 hours, but the frequency or time/day are configurable.
   2. ossec-syscheckd is able to check file integrity in near realtime on Windows and modern Linux distros. Windows comes with support out of the box, but on Linux systems inotify packages may need to be installed. Check for inotify dev packages, and possibly an inotify-tools package. These configuration options can be specified in each agent’s ossec.conf file, except for the auto\_ignore and alert\_new\_file which apply to manager and local installs. The ignore option applies to all agents if specified on the manager.
   3. Use this ‘directories’ option to add or remove directories to be monitored (they must be comma separated). All files and subdirectories will also be monitored. Drive letters without directories are not valid. At a minimum the ‘.’ should be included (D:\.). This should be set on the system you wish to monitor (or in the agent.conf if appropriate).
5. How do levels work with OSSEC rules?

The rules will be read from the highest to the lowest level.

00 - Ignored - No action taken. Used to avoid false positives. These rules are scanned before all the others. They include events with no security relevance.

01 - None -

02 - System low priority notification - System notification or status messages. They have no security relevance.

03 - Successful/Authorized events - They include successful login attempts, firewall allow events, etc.

04 - System low priority error - Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.

05 - User generated error - They include missed passwords, denied actions, etc. By itself they have no security relevance.

06 - Low relevance attack - They indicate a worm or a virus that have no affect to the system (like code red for apache servers, etc). They also include frequently IDS events and frequently errors.

07 - “Bad word” matching. They include words like “bad”, “error”, etc. These events are most of the time unclassified and may have some security relevance.

08 - First time seen - Include first time seen events. First time an IDS event is fired or the first time an user logged in. If you just started using OSSEC HIDS these messages will probably be frequently. After a while they should go away, It also includes security relevant actions (like the starting of a sniffer or something like that).

09 - Error from invalid source - Include attempts to login as an unknown user or from an invalid source. May have security relevance (specially if repeated). They also include errors regarding the “admin” (root) account.

10 - Multiple user generated errors - They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credencials.

11 - Integrity checking warning - They include messages regarding the modification of binaries or the presence of rootkits (by rootcheck). If you just modified your system configuration you should be fine regarding the “syscheck” messages. They may indicate a successful attack. Also included IDS events that will be ignored (high number of repetitions).

12 - High importancy event - They include error or warning messages from the system, kernel, etc. They may indicate an attack against a specific application.

13 - Unusual error (high importance) - Most of the times it matches a common attack pattern.

14 - High importance security event. Most of the times done with correlation and it indicates an attack.

15 - Severe attack - No chances of false positives. Immediate attention is necessary.

1. Review the rootkit\_trojans.txt file in /var/ossec/etc/shared. Why is OSSEC looking for antivirus sites in /etc/hosts?
   1. Malware uses /etc/hosts for their own reasons, where the two most common ones are:
      1. To block detection by security software: for example, by blocking the traffic to all the download or update servers of the most well-known security vendors.
      2. To redirect traffic to servers of their choice: for example, by intercepting traffic to advertisement servers and replacing the advertisements with their own.
2. After OSSEC is running on your machine for a few hours/days, what kind of alerts are you experiencing?
   1. Example alert.log messages:

\*\* Alert 1510376401.0: - syslog,errors,

2017 Nov 11 00:00:01 ix->/var/log/messages

Rule: 1005 (level 5) -> 'Syslogd restarted.'

Nov 11 00:00:01 ix syslogd[72090]: restart

\*\* Alert 1510376417.172: - syslog,smtpd,

2017 Nov 11 00:00:17 (junction) 192.168.17.17->/var/log/maillog

Rule: 53508 (level 5) -> 'Server TLS certificate verification failed.'

Nov 11 00:00:16 junction smtpd[86532]: smtp-out: Server certificate verification failed on session 99fc1afc58067419

\*\* Alert 1510376428.465: - syslog,sudo

2017 Nov 11 00:00:28 ubnt->/var/log/syslog-ng/messages

Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'

User: root

Nov 5 15:35:03 ubnt sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/vtysh.pl -c show ip route summary json

\*\* Alert 1510376428.758: - pam,syslog,authentication\_success,

2017 Nov 11 00:00:28 ubnt->/var/log/syslog-ng/messages

Rule: 5501 (level 3) -> 'Login session opened.'

Nov 5 15:35:03 ubnt sudo: pam\_unix(sudo:session): session opened for user root by (uid=0)